AFA ZW

PTO/SB/21
0018.0056

TRANSMITTAL FORM	Application Number	09/409,617
(To be used for all correspondence after initial filing)	Filing Date	October 1, 1999
	Inventor	D.M. SHACKELFORD
	Group Art Unit	2132
	Examiner Name	Benjamin E. Lanier
Total Number of Pages in this Submission:	Attorney Docket Number	TU999029

ENCLOSURES *(check all that apply)*

☒ Fee Transmittal Form ☐ Fee Attached ☐ Amendment/Reply ☐ After Final ☐ Affidavits /Declarations ☐ Extension of Time Request ☐ Express Abandonment Request ☐ Information Disclosure Statement; ___ references ☐ Certified Copy of Priority Document(s) ☐ Response to Missing Parts/Incomplete Application ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53	☐ Assignment Papers (for an application) ☐ Formal Drawings: ___ sheets ☐ Licensing-related papers ☐ Petition: _____ ☐ Petition to Convert to a Provisional Application ☐ Power of Attorney, Revocation, and/or Change of Correspondence Address ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) __ ☐ After Allowance Communication to Group	☐ Certificate of Correction of Applicant's Mistake (37 CFR 1.323) ☐ Certificate of Correction of Office Mistake (37 CFR 1.322) ☒ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)* 31 pages ☐ Proprietary Information ☐ Status Letter ☐ Appeal Communication to Board of Appeals and Interferences ☐ Fee Address Indication Form ☐ Other Enclosure(s) *(please identify below)*

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual Name:	David W. Victor, Registration No. 39,867
Signature:	/David Victor/
Date:	June 12, 2006
KONRAD RAYNES & VICTOR, LLP 315 South Beverly Drive, Suite 210 Beverly Hills, California 310-556-7983	The Commissioner is authorized to charge to Deposit Account No. 09-0449 any additional fee required under 37 CFR 1.16 and 1.17, including all required extension of time fees, and charge any other deficiency or credit any overpayment to this deposit account.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

Typed or Printed name:	David W. Victor	Customer No. **46917**
Signature:	/David Victor/	
Date:	June 12, 2006	

PTO/SB/17
0018.0056

FEE TRANSMITTAL for FY 2005		
	Application Number	09/409,617
	Filing Date	October 1, 1999
	Inventor	D.M. SHACKELFORD
	Group Art Unit	2132
	Examiner Name	Benjamin E. Lanier
Total Amount of Payment: **$500.00**	Attorney Docket Number	TU999029

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge the indicated fees and/or credit any overpayments to Deposit Account Number: 09-0449
☒ Charge any additional fee required under 37 CFR 1.16 and 1.17, including all required extension of time fees.
☒ Charge any deficiency or credit any overpayment

2. ☐ Payment enclosed:
   - ☐ Ck. No. _____ for $_____
   - ☐ Ck. No. _____ for $40
   - ☐ Credit Card Approval for_____

FEE CALCULATION

1. ☒ BASIC FILING FEE Utility Filing Fee: Large Entity Fee Code 1011	$300.00
2. ☒ UTILITY SEARCH FEE	$500.00
3. ☒ UTILITY EXAMINATION FEE	$200.00
4. ☒ EXTRA CLAIMS FEES Total Claims ___ - 20* x $50= Ind. Claims ___ - 3* x $200= Multiple Dependent 0 x $360=	$_____ $_____ $0
Subtotal	$_____

*(or number previously paid for)

FEE CALCULATION (continued)

3. ADDITIONAL FEES (large entity)	
☐ Surcharge- late filing fee or oath	$130
☐ Surcharge- late provisional filing fee or cover sheet	$50
☐ Non-English specification	$130
☐ International type search report	$40
☐ Requesting publication of SIR prior to action	$920
☐ Requesting publication of SIR after action	$1840
☐ Extension for reply- first month	$120
☐ Extension for reply- second month	$450
☐ Extension for reply- third month	$1020
☐ Extension for reply- fourth month	$1590
☐ Extension for reply- fifth month	$2160
☐ Notice of Appeal	$500
☒ Brief in Support of Appeal	$500
☐ Request for Oral Hearing	$1000
☐ Utility issue fee	$1400
☐ Petition to revive (unavoidable)	$500
☐ Petition to revive (unintentional)	$1500
☐ Petitions to the Commissioner	$130
☐ Petitions related to provisional applications	$50
☐ Submission of Information Disclosure Statement	$180
☐ Recordation of Assignment	$40
☐ Submission after final (37 CFR 1.129(a))	$790
☐ Request for Continued Examination (RCE)	$790
☐ Other:	
SUBTOTAL	$ 500

Submitted by:

Firm or Individual Name:	David W. Victor; Registration No. 39,867	Customer No. 46917
Signature:	/David Victor/	
Date: June 12, 2006	Telephone: (310) 553-7977	

In the United States Patent and Trademark Office
Board of Patent Appeals and Interferences

Appeal Brief

In re the Application of:

David Michael SHACKELFORD
Serial No. 09/409,617
Filed: October 1, 1999
Attorney Docket No. TU999029

METHOD, SYSTEM, AND PROGRAM FOR DISTRIBUTING SOFTWARE BETWEEN COMPUTER SYSTEMS

Submitted by:

Konrad, Raynes & Victor LLP
315 So. Beverly Dr., Ste. 210
Beverly Hills CA 90212
(310) 556-7983
(310) 556-7984 (fax)

TABLE OF CONTENTS

I. Real Party in Interest

The entire right, title and interest in this patent application is assigned to real party in interest International Business Machines Corporation.

II. Related Appeals, Interferences, and Judicial Proceedings

Appellant, Appellant's legal representative, and Assignee are not aware of any other prior or pending appeals, interferences, and judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of the Claims

Claims 1-40 are pending and have been rejected.

The final rejection of the claims in the Final Office Action dated December 13, 2005 (Dec. 2005 FOA) is being appealed for all pending claims 1-40.

IV. Status of Amendments

No amendment was filed after receipt of the Final Rejection from which this Appeal was taken.

V. Summary of the Claimed Subject Matter

Independent claims 1, 16, and 27 concern distributing computer software from a first computer system. With respect to the preamble, the Specification discloses that a software company may manage a source system 2 (FIG. 1) to provide a software package 4 for installation and use on hardware from companies that are licensees. (Specification, pg. 5, lines 13-16). Below is an explanation of the claimed subject matter referring to the specification and drawings, where the claim requirements for the first computer system are underlined:

> maintaining keys of computer systems authorized to access software to be distributed. With respect to this requirement, the Specification discloses that the source system 2 includes the public keys K(T)s of all systems authorized to access

the software , such as public key 14 K(T). (Specification, pg. 6, lines 14-19, FIG. 1).

receiving a request for software from a second computer system. With respect to this requirement, the Specification discloses that at block 100 in FIG. 2, the source system 2 receives a request for the software package 4 from the target 8. (Specification, pg. 7, lines 4-7 and FIG. 2, block 100).

generating a message. With respect to this requirement, the Specification discloses that the source system 2 generates at block 104 a random message (R). (Specification, pg. 7, lines 7-10 and FIG. 2, block 104).

encrypting the generated message. With respect to this requirement, the Specification discloses that the source system 2 encrypts at block 106 the generated random message (R) with its private key J(S) to produce the encrypted message. (Specification, pg. 7, lines 10-12 and FIG. 2, block 106).

transmitting the encrypted message to the second computer system. With respect to this requirement, the Specification discloses that the source system 2 transmits the encrypted message at block 108 to the target system. (Specification, pg. 7, lines 12-13 and FIG. 2, block 108).

receiving an encrypted response from the second computer system. With respect to this requirement, the Specification discloses that the source system 2 receives the encrypted message from the target system 8 at block 110 in FIG. 2. (Specification, pg. 7, lines 24-25 and FIG. 2, block 110).

determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response. With respect to this requirement, the Specification discloses that the source system 2 determines at block 112 in FIG. 2 whether it has one target public key K(T) that can decrypt the message. (Specification, pg. 7, lines 24-26 and FIG. 2, block 112).

decrypting the encrypted response with the determined key if there is one determined key. With respect to this requirement, the Specification discloses that if the source system 2 can decrypt, then the source system 2 determines whether the decrypted message matches a previously transmitted random message (Specification, pg. 7, line 27 to pg. 8, line 2 and FIG. 2, block 116).

determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the generated message transmitted to the second computer system. With respect to this requirement, the Specification discloses that if the source system 2 can decrypt, then the source system 2 determines whether the decrypted message matches a previously transmitted random message. If the decrypted message matches, then the software package is returned at block 118 in FIG. 2 or if the message cannot be decrypted or the decrypted message does not match previously transmitted message, then the verification program ends at block 114 in FIG. 2 without providing the program. (Specification, pg. 7, line 27 to pg. 8, line 16 and FIG. 2, blocks 112-118).

permitting the second computer system access to the software after determining that the second computer system is authorized to access the software: With respect to this requirement, the Specification discloses that if the decrypted message matches, then the software package is returned at block 118 (Specification, pg. 7, line 27 to pg. 8, line 16 and FIG. 2, blocks 112-118).

Independent claim 16 recites each of the above functional requirements with "means" language. The structure, material or acts described in the Specification corresponding to these "means" functions comprise the source system 2 in FIG. 1, which performs the operations of FIG. 2. (Specification, pg. 7, lines 1-4). The Specification discloses that in embodiments the source system 2 comprises a server suited for distributing software. (Specification, pg. 5, lines 7-12)

The patentability of claim 22, which depends from base claim 16, is argued separately. Claim 22 includes recitation of "means" language. The structure, material or acts described in the Specification corresponding to these "means" functions comprise

the source system 2 in FIG. 1, which performs the operations of FIG. 2. (Specification, pg. 7, lines 1-4, pg. 5, lines 7-12)

Independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system. With respect to the preamble, the Specification discloses allowing purchasers of hardware from licenses to access and install software package on hardware. (Specification, pg. 5, lines 15-16). Below is an explanation of the claimed subject matter referring to the specification and drawings, where the claim requirements of the second computer system are underlined:

providing a key to the first computer system capable of decrypting an encrypted response from the from the second computer system. With respect to this requirement, the Specification discloses that source system 2 maintains a target public key K(T) for each target system authorized to access the software. The source 2 and target 8 systems include each other's public/private key pair to send messages and use public key cryptography standards known in the art. A user maintains a private key and distributes public keys to others. The user can then encrypt message s with the private key and send to others having the public key. (Specification, pg. 5, lines 17-25 and pg. 9, lines 17-21)

transmitting a request for the software to the first computer system. With respect to this requirement, the Specification discloses that at block 150 in FIG. 3, the target system 8 generates and sends a request for the software package 4 to the source system 2. (Specification, pg. 7, lines 4-6).

receiving an encrypted message from the first computer system. With respect to this requirement, the Specification discloses that at block 160 in FIG. 3, the target system 8 receives the encrypted message from the source system 2. (Specification, pg. 7, lines 14-15)

processing the encrypted message to generate a response message. With respect to this requirement, the Specification discloses at block 162 in FIG. 3 that the target system 8 decrypts the message using the source system's public key K(S) to produce message (R). (Specification, pg. 7, lines 15-16).

encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system.

With respect to this requirement, the Specification discloses at block 164 in FIG. 3 that the target system encrypts the message (R) using its private key J(T). This message can be decrypted with the target public key K(T). (Specification, pg. 7, lines 22-26)

transmitting the encrypted response message to the first computer system. With respect to this requirement, the Specification discloses at block 166 in FIG. 3 that the target system 8 transmits the encrypted message to the source system 2. (Specification, pg. 7, line 23)

receiving access to the requested software in response to the encrypted response message With respect to this requirement, the Specification discloses that the source system 2 returns the software package 4 to the target system 8 if the encrypted response message can be decrypted and matches. (Specification, pg. 7, lines 24 to pg. 8, line 16, FIG. 2, blocks 110-118).

Independent claim 25 recites the above requirements in "means" form. The structure, material or acts described in the Specification corresponding to these claimed "means" functions comprise the target system 8 in FIG. 1, which performs the operations of FIG. 3. (Specification, pg. 7, lines 1-4). The Specification discloses that in embodiments the target system comprises any computer device connected to the network that is authorized to access and install the software package 4. (Specification, pg. 5, lines 17-20)

VI. Grounds of Rejection to Be Reviewed on Appeal

A concise statement listing each ground of rejection presented for review is as follows:

A. Claims 1, 2, 8-14, 16, 17, 21-28, and 34-40 are rejected under 35 U.S.C. §102 as being unpatentable over Davis (U.S. Patent No. 5,473,692).

B. Claims 3, 18, and 29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Davis.

C. Claims 4, 15, 19, and 30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Schneier ("Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C" by Bruce Schneier, 1996).

D. Claims 5, 6, 31, and 32 are rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Komura (U.S. Patent No. 5,994,307).

E. Claims 7, 20, and 33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Takahashi (U.S. Patent No. 6,195,432).

VII. Argument

A. Rejection Under 35 U.S.C. §102 Over Davis

1. Claims 1, 2, 8-11, 16, 17, 21-24, 27, 28, and 34-40

Independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: maintaining keys of computer systems authorized to access software to be distributed; receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined key if there is one determined key; determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the generated message transmitted to the second computer system; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

The Examiner cited col. 7, lines 30-64 of Davis as disclosing the requirement of the first computer system that distributes software maintaining keys of computer systems

authorized to access software the software to be distributed. (Dec. 2005 FOA, pg. 2) Applicants traverse this finding.

The cited col. 7 discusses how to generate a unique public/private key pair. A hardware agent establishes a coupling with a certification system, which has a database of previously generated public keys to guarantee unique key generation. After the hardware agent generates the public/private key pair, the pair is transmitted to the certification system to determine whether the generated public key is unique.

Nowhere does this cited col. 7 anywhere disclose the claim requirement of a first computer system that distributes software maintaining keys of computer systems authorized to access software to be distributed. Instead, the cited col. 7 discusses a certification system that stores public keys to make sure that a new public key that is generated is unique, i.e., does not match a previously generated key. Further, the public keys maintained by the cited certification system are public keys generated for systems, not keys of computer systems authorized to access software to be distributed as claimed.

The Examiner cited col. 8, lines 54-58 of Davis as disclosing the claim requirements of determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined key if there is one determined key. (Feb. 2005 FOA, pg. 3) Applicants traverse.

The cited col. 8 discusses how a first hardware agent is authenticated with a second hardware agent. The second hardware agent transmits a challenge/response message to the first hardware agent. The first hardware agent decrypts the challenge/response message with its private key and generates a response encrypting the decrypted challenge message with the public key of the second hardware agent. The second hardware agent decrypts the response with its private key and compares the original challenge message to the decrypted response from the first hardware agent. (Davis, col. 8, lines 45-60).

Nowhere does the cited Davis anywhere disclose that the second hardware agent doing the authentication, corresponding to the claimed first computer system, determine whether there is one key for the second computer system (corresponding to the cited first hardware agent) that can be used to decrypt the message and then decrypting the

encrypted response from the claimed second computer system with that determined key. In the cited Davis, the cited second hardware agent does not need to determine whether there is one maintained key for the first hardware agent in order to decrypt the message having the challenge/response because the message was encrypted with the public key of the receiving second hardware agent, not a key specific to the first hardware agent. Thus, in the cited Davis, the second hardware agent (claimed first computer system) uses its own private key to decrypt the response having the challenge response, not a maintained key for the first hardware agent (claimed second computer system requesting software).

In other words, nowhere does the cited Davis anywhere disclose the claim requirement of determining a key for the second computer system to use to decrypt the message. Instead, the cited Davis has the second hardware agent, corresponding to the claimed first computer system, use its own private key to decrypt the response having the challenge message, not a key maintained for the sending first hardware agent, corresponding to the second computer system.

In the Advisory Action dated March 2, 2006, the Examiner cited col. 5, lines 40-46 as teaching the claim requirement of the first computer system decrypting the response from the second computer system with one key maintained for the second computer system. (Advisory Action, Continuation Sheet).

The cited col. 5 mentions that a message digest is encrypted using a private key of the first node (PRK1) and that a symmetric key is encrypted with a public key of the second node (PUK2), both inputted into a transmission message. The second node decrypts using its private key (PRK2) and a published key (PUBTA) of the trusted authority to obtain the secret key and public key (PUK1). The SK and PUK1 keys are used to decrypt the encrypted message to retrieve the message digest.

The cited col. 5 discusses how a second node uses a public key to decrypt a message decrypted using a private key of the first node (PRK1). However, there is no disclosure in this cited section of the claim requirement that the second node (corresponding to the claimed first computer system) determine whether there is a key maintained for the second computer system to decrypt a received response, such that the second computer system (cited first node) is not allowed to access software if there is no determined key for the second computer system, i.e., first node.

In the Advisory Action, the Examiner further found that the public key of the first node PUK1 meets the limitation of determining whether there is one maintained key of the second computer system capable of decrypting the received response. Applicants traverse on the ground that according to the cited col. 5 the cited second node does not determine whether there is one maintained key for the first node (second computer system) as claimed. Instead, according to the cited col. 5, the second node decrypts the symmetric key (SK) and the digital certificate with a published key (PUBTA) of a trusted authority to obtain the public key of the first node (PUK1). (Davis, col. 5, lines 47-56) Thus, the second node does not maintain keys as claimed of systems authorized to access software as claimed, because the second node obtains the public key of the first node from a trusted authority. Moreover, there is no disclosure that the cited second node considers the presence or absence of a key for the first node to determine whether to authorize the first node to access software. Instead, the cited second node uses a published key (PUBTA) to obtain the public key, not determine whether there is a key from the first node from maintained keys of nodes or systems authorized to access the software.

The Examiner cited col. 8, lines 60-65 and col. 9, lines 15-22 of Davis as disclosing the claim requirement that the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response. (Dec. 2005 FOA, pg. 3) The cited col. 8 does not disclose this requirement because the cited second hardware agent (corresponding to the claimed first computer system) does not use the presence of a key maintained for the first hardware agent to determine whether access to software is permitted. In fact, the presence of a key for the first hardware agent (second computer system) is not at issue in the cited col. 8 because the second hardware agent (first computer system) uses its own private key to decrypt the message, not a key maintained for the first hardware agent as claimed. Further, according to the cited col. 8, the second hardware agent authenticates the message based on the presence of the proper challenge response, not the availability of a key maintained for the first hardware agent.

Moreover, the cited col. 8 discusses how the cited challenge/response technique is used to verify that both hardware agents are authentic and communication is secure.

(Davis, col. 8, line 65 to col. 9, line 9). This cited challenge/response technique in col. 8 is not done to determine whether one node, i.e., the claimed second computer system, is authorized to access software.

The cited col. 9, lines 15-22 of Davis discusses a process of the first hardware agent to determine whether the second hardware agent has a valid license "after secure communications are established" using the challenge/response technique discussed above. (Davis, col. 9, lines 5-13). Thus, the above discussed challenge/response technique the Examiner cited as disclosing determining whether a computer is authorized to access software is performed not to determine whether a computer is authorized to access software as claimed, but is instead performed to "secure communications" between the agents.

Moreover, the cited col. 9 mentions that the first hardware agent initiates a request for the license token to operate the software if the second hardware agent has a valid license token. Nowhere does this cited col. 9 disclose the above discussed requirements for determining whether the second computer system is authorized to access the software based on the presence of one maintained key for the second computer system requesting access. Instead, the cited col. 9 discusses a process where one hardware agent requests a license token from another to use software.

In other words, the challenge/response technique of the cited col. 8 is for the purpose of establishing secure communications. After, communications are secure, the cited col. 9 discusses how a first hardware agent may request a valid license token from the second to operate the software. Nowhere do these cited cols. 8 and 9 of Davis disclose that a first computer system maintains keys of computer systems authorized to access the software, where the keys are used to determine whether a computer system is authorized to access the software. Instead, the above discussed Davis discusses how the second hardware agent, authenticating the first, uses its own private key to decrypt the message, not a key maintained for the first hardware agent requesting access or authentication.

For all the above reasons, Applicants request reversal of the rejection of claims 1, 16, and 27 because the cited Davis does not disclose all the claim requirements.

Claims 2, 8, 17, 21, 28, 34, 38-40 are patentable over the cited art because they depend from one of claims 1, 16, and 27

2. Claims 12-14, 25, and 26

Independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system and require that the second computer system perform: providing a key to the first computer system capable of decrypting an encrypted response from the from the second computer system; transmitting a request for the software to the first computer system; receiving an encrypted message from the first computer system; processing the encrypted message to generate a response message; encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system; transmitting the encrypted response message to the first computer system; and receiving access to the requested software in response to the encrypted response message.

The Examiner cited the above discussed sections of Davis cited with respect to independent claims 1, 16, and 27 in rejecting independent claims 12 and 25. (Dec. 2005 FOA, pgs. 4-5). Applicants traverse for the following reasons.

Applicants submit that nowhere does the cited Davis disclose that the a second computer system (requesting access to the software) encrypts a response message to the first computer system, wherein the first computer may use a key provided by the second computer system to decrypt the response message to receive access to requested software in response to the encrypted response message.

The cited col. 8 of Davis mentions that the first hardware agent (requesting authorization) encrypts a response comprising the decrypted challenge message with the public key of the second hardware agent. (Davis, Col. 8, lines 50-60) Nowhere does the cited Davis disclose that the first hardware agent (corresponding to the claimed second computer system) encrypts the challenge message that can be decrypted with a key the first hardware agent provided to the second hardware agent (corresponding to the claimed first computer system). Instead, in the cited Davis, the first hardware agent encrypts the message so that it may be decrypted with the private key of the second hardware agent,

not with a key the second computer system provides to the first computer system as claimed.

Moreover, as discussed, the challenge/response procedure of the cited col. 8 is for the purpose of ensuring secure communications between the hardware agents. The claims require that the second computer system receives access to the software in response to the encrypted response message. Nowhere does this cited col. 8 disclose that one agent receive access to requested software in response to the cited challenge/response procedure.

The cited col. 9 discusses how a first hardware agent may request a valid license token from the second to operate the software. Nowhere does the cited col. 9 disclose that the second computer system encrypt a response message capable of being decrypted by a key the second computer system provided to the first computer system to receive access to requested software. Moreover, when discussing encrypting response messages, the above discussed Davis discusses how the second hardware agent, authenticating the first, uses its own private key to decrypt the message, not a key maintained for the first hardware agent requesting access to the software.

Accordingly, Applicants request reversal of the rejection of claims 12 and 25 are patentable because the cited Davis does not disclose all the claim requirements.

Claims 13, 14, 26 are patentable over the cited art because they depend from one of claims 12 and 25.

3. Claims 9, 22, and 35

Claims 9, 22, and 35 depend from claims 8, 21, and 34 and further require that encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise public keys from the authorized computer systems, wherein

processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

The Examiner cited the above discussed sections of Davis as disclosing the additional requirements of these claims. (Dec. 2005 FOA, pgs. 5-6) Applicants traverse.

The claims require that the first computer system maintain public keys from authorized computer systems and use the requesting second computer system's public key to decrypt the response with the maintained public key. The cited col. 8 of Davis mentions that the second hardware agent (corresponding to the claimed first computer system) decrypts the message from the first hardware agent (corresponding to the claimed second computer system) including the challenge response with its own private key. The cited Davis does not disclose that the second hardware agent decrypts the message including the challenge response with a determined public key from the second computer system requesting access to the software. Further, nowhere does the cited Davis disclose that the second hardware agent maintain public keys from multiple authorized first hardware agents to use to decrypt their challenge response.

The cited col. 9 discusses how one agent requests a valid license token to operate the software from another agent. Nowhere does the cited Davis disclose that as part of this request for the valid license token, the requesting agent (corresponding to the claimed first computer system) decrypt the request for the license token with a determined public key from the second computer system requesting access to the software or the license token.

Applicants request reversal of the rejections of claims 9, 22, and 35 on the grounds that the additional requirements of these claims are not disclosed in the cited Davis, thus providing additional grounds of patentability over the cited art.

4. Claims 10, 11, 23, 24, 36, and 37

Claims 10, 23, and 36 depend from claims 1, 16, and 27 and further require that the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

The Examiner cited col. 8, lines 33-35 of Davis as disclosing the limitation of configuration data of these claims. (Dec. 2005 FOA, pg. 6)

The cited col. 8 mentions that the first hardware agent, requesting authentication, outputs a message including its unique authentication device certificate to the second hardware agent. The second hardware agent uses this authentication device certificate to obtain the public key (PUKM) of the first hardware agent.

The Examiner found that this cited Davis discloses that the challenge includes the digital certificate to meet the requirement of configuration data. (Dec. 2005 FOA, pg. 6) Applicants traverse.

The cited col. 8 discusses one agent submitting an authentication device certificate to allow the other agent to obtain the public key of the submitting agent. The discussion at col. 8, lines 45-67 of the challenge/response does not describe that the cited authentication certificate is included in the challenge/response. Instead, the cited authentication certificate is sent to allow the receiver to obtain the public key of the sender.

Moreover, nowhere does this cited col. 8 anywhere disclose that the message sent with the authentication certificate include a request for configuration data from the second hardware agent (corresponding to the claimed second computer system), such that a determination is made whether the configuration data is for a system that is authorized to access the software. Instead, the cited col. 8 mentions a unique device certificate, not a request and consideration of configuration data of the requesting system (first hardware agent) as claimed.

Applicants request reversal of the rejection of claims 10, 23, and 36 on the grounds that the additional requirements of these claims are not disclosed in the cited Davis, thus providing additional grounds of patentability over the cited art.

B. Rejection Under 35 U.S.C. §103(a) Over Davis

1. Claims 3, 18, and 29

Applicants request reversal of the rejection of claims 3, 18, and 29 over the cited art because they depend from claims 1, 16, and 27, respectively, which are patentable over the cited art for the reasons discussed above.

C. Rejection Under 35 U.S.C. §103(a) Over Davis in View of Schneier

1. Claims 4, 15, 19, and 30

Applicants request reversal of the rejection of claims 4, 15, 19, and 30 over the cited art because they depend from one of claims 1, 12, 16, and 27, respectively, which are patentable over the cited art for the reasons discussed above.

D. Rejection Under 35 U.S.C. §103(a) Over Davis in View of Komura

1. Claims 5, 6, 31, and 32

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited col. 7, lines 22-30 and col. 6, lines 40-67 of Komura as teaching the time stamp claim requirement. (Dec. 2005, FOA, pg. 10) Applicants traverse.

The cited cols. 6 and 7 of Komura discusses how a time stamp is attached to a packet and how the time stamp is used. However, Komura concerns the use of a time stamp with a packet for communicating the packet. (Komura, col. 1, lines 5-12). Nowhere does the cited Komura teach or suggest the use of a time stamp as a random component used to determine whether a second computer system may access software. Instead, the time stamp of Komura is used for transmitting a packet without stopping even when a bit rate becomes higher. (Komura, col. 1, lines 5-12).

Applicants request reversal of the rejection of claims 5 and 31 on the grounds that the additional requirements of these claims are not disclosed in the cited Komura, thus providing additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons discussed above, i.e., because Komura does not teach the use of a time stamp to determine whether a second computer system can access software.

Applicants request reversal of the rejection of claims 6 and 32 on the grounds that the additional requirements of these claims are not disclosed in the cited Komura, thus providing additional grounds of patentability over the cited art.

E. Rejection Under 35 U.S.C. §103(a) Over Davis in View of Takahashi

1. Claims 7, 20, and 33

Applicants request reversal of the rejection of claims 7, 20, and 33 over the cited art because they depend from one of claims 1, 16, and 27, respectively, which are patentable over the cited art for the reasons discussed above.

VIII. Conclusion

Each of the rejections set forth in the Final Office Action is improper and should be reversed.

Respectfully submitted,

/David Victor/

David W. Victor
Reg. No. 39,867

Dated: June 12, 2006

Direct All Correspondence to:
David Victor
Konrad Raynes & Victor LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, California 90212
Tel: 310-553-7977
Fax: 310-556-7984

IX. Claims Appendix

1. (Previously Presented) A method for distributing computer software from a first computer system, comprising the first computer system performing:

maintaining keys of computer systems authorized to access software to be distributed;

receiving a request for software from a second computer system;

generating a message;

encrypting the generated message;

transmitting the encrypted message to the second computer system;

receiving an encrypted response from the second computer system;

determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response;

decrypting the encrypted response with the determined key if there is one determined key;

determining whether the decrypted response includes a part of the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the part of the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the part of the generated message transmitted to the second computer system; and

permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

2. (Original) The method of claim 1, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

3. (Original) The method of claim 1, further comprising transmitting the software to the second computer system after permitting access.

4. (Previously Presented) The method of claim 1, wherein generating the message further comprises generating a random component to include within the message, and wherein determining whether the decrypted response includes the part of the generated message comprises determining whether the decrypted response includes the random component.

5. (Previously Presented) The method of claim 4, wherein the random component is comprised of a time stamp.

6. (Previously Presented) The method of claim 4, wherein the time stamp is inserted at an offset into the message.

7. (Original) The method of claim 1, wherein the software comprises a computer program, further comprising automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

8. (Original) The method of claim 1, wherein processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

9. (Previously Presented) The method of claim 8, wherein encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise

public keys from the authorized computer systems, wherein processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

10. (Original) The method of claim 1, wherein the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

11. (Previously Presented) The method of claim 10, wherein the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system, and wherein the encrypted response is encrypted with a private key of the second computer system, wherein the maintained keys comprise public keys from authorized computer systems.

12. (Previously Presented) A method for accessing computer software from a first computer system with a second computer system, wherein the second computer system performs:

providing a key to the first computer system capable of decrypting an encrypted response from the second computer system;

transmitting a request for the software to the first computer system;

receiving an encrypted message from the first computer system;

processing the encrypted message to generate a response message including a part of the encrypted message;

encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system;

transmitting the encrypted response message to the first computer system; and

receiving access to the requested software in response to the encrypted response message.

13. (Original) The method of claim 12, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

14. (Previously Presented) The method of claim 12, wherein the received encrypted message is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, further comprising;

decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key;

encrypting the decrypted message with the second computer system's private key; and

transmitting the message encrypted with the second computer system's private key to the first computer system, wherein the key made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

15. (Original) The method of claim 12, wherein the received encrypted message includes a random component and a request for configuration data from the second computer system, further comprising adding configuration data for the second computer system to the decrypted message before encrypting the message with the second computer system's private key.

16. (Previously Presented) A system for distributing computer software from a first computer system to a second computer system, wherein the first computer comprises:

means for maintaining keys of computer systems authorized to access software to be distributed;

means for receiving a request for software from the second computer system;

means for generating a message;

means for encrypting the generated message;

means for transmitting the encrypted message to the second computer system;

means for receiving an encrypted response from the second computer system;

means for determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response;

means for decrypting the encrypted response with the determined key if there is one determined key;

means for determining whether the decrypted response includes a part of the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the part of the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the part of the generated message transmitted to the second computer system; and

means for permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

17. (Original) The system of claim 16, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

18. (Original) The system of claim 16, further comprising means for transmitting the software to the second computer system after permitting access.

19. (Previously Presented) The system of claim 16, wherein the means for generating the message further comprises generating a random component to include within the message, and wherein the means for determining whether the decrypted response includes the part of generated message comprises determining whether the decrypted response includes the random component.

20. (Original) The system of claim 16, wherein the software comprises a computer program, further comprising means for automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

21. (Original) The system of claim 16, wherein the means for processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

22. (Previously Presented) The system of claim 21, wherein the means for encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise public keys from the authorized computer systems, wherein the means for processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

23. (Original) The system of claim 16, wherein the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

24. (Previously Presented) The system of claim 23, wherein the generated message is encrypted with a private key of the first computer system, wherein the first

computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system, and wherein the encrypted response is encrypted with a private key of the second computer system, wherein the maintained keys comprise public keys from authorized computer systems.

25. (Previously Presented) A system for accessing computer software from a first computer system with a second computer system, wherein the second computer system comprises:

means for providing a key to the first computer system capable of decrypting an encrypted response from the second computer system;

means for transmitting a request for the software to the first computer system;

means for receiving an encrypted message from the first computer system;

means for processing the encrypted message to generate a response message including a part of the encrypted message;

means for encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided key at the first computer system;

means for transmitting the encrypted response message to the first computer system; and

means for receiving access to the requested software in response to the encrypted response message.

26. (Previously Presented) The system of claim 25, wherein the received encrypted message is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, further comprising;

means for decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key;

means for encrypting the decrypted message with the second computer system's private key; and

means for transmitting the message encrypted with the second computer system's private key to the first computer system, wherein the key made available by the second computer system that is capable of decrypting the received encrypted response comprises a public key associated with the second computer system.

27. (Previously Presented) An article of manufacture for use in distributing computer software from a first computer system the article of manufacture comprising computer usable media including at least one computer program embedded therein that causes the first computer system to perform:

maintaining keys of computer systems authorized to access software to be distributed;

receiving a request for software from a second computer system;

generating a message;

encrypting the generated message;

transmitting the encrypted message to the second computer system;

receiving an encrypted response from the second computer system;

determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response;

decrypting the encrypted response with the determined key if there is one determined key;

determining whether the decrypted response includes a part of the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the part of the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the part of the generated message transmitted to the second computer system; and

permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

28. (Original) The article of manufacture of claim 27, wherein the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

29. (Original) The article of manufacture of claim 27, further comprising transmitting the software to the second computer system after permitting access.

30. (Previously Presented) The article of manufacture of claim 27, wherein generating the message further comprises generating a random component to include within the message, and wherein determining whether the decrypted response includes the generated message comprises determining whether the decrypted response includes the random component.

31. (Previously Presented) The article of manufacture of claim 30, wherein the random component is comprised of a time stamp.

32. (Previously Presented) The article of manufacture of claim 31, wherein the time stamp is inserted at an offset into the message.

33. (Original) The article of manufacture of claim 27, wherein the software comprises a computer program, further comprising automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

34. (Original) The article of manufacture of claim 27, wherein processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

35. (Previously Presented) The article of manufacture of claim 34, wherein encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise public keys from the authorized computer systems, wherein processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

36. (Previously Presented) The article of manufacture of claim 27, wherein the generated message includes a random component and a request for configuration data from the second computer system, wherein processing the encrypted response comprises determining whether the response includes configuration data for a system that is authorized to access the computer software.

37. (Previously Presented) The article of manufacture of claim 36, wherein the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system, and wherein the encrypted response is encrypted with a private key of the second computer system, wherein the maintained keys comprise public keys from authorized computer systems.

38. (Original) The article of manufacture of claim 27, the article of manufacture comprising at least one additional software program to cause the second computer system to perform:

transmitting a request for the software to the first computer system;

receiving an encrypted message from the first computer system;

processing the encrypted message to generate a response message;

transmitting the response message to the first computer system; and

receiving access to the requested software in response to the response message.

39. (Previously Presented) The article of manufacture of claim 38, wherein the received encrypted message is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, further comprising;

decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key;

encrypting the decrypted message with the second computer system's private key; and

transmitting the message encrypted with the second computer system's private key to the first computer system, wherein the key made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

40. (Original) The article of manufacture of claim 38, wherein the received encrypted message includes a random component and a request for configuration data from the second computer system, further comprising adding configuration data for the second computer system to the decrypted message before encrypting the message with the second computer system's private key

X. Evidence Appendix

None

XI. Related Proceedings Appendix

None